CRITICAL INFRASTRUCTURE PROTECTION

Capability Definition

The Critical Infrastructure Protection (CIP) capability enables public and private entities to identify, assess, prioritize, and protect critical infrastructure and key resources so they can detect, prevent, deter, devalue, and mitigate deliberate efforts to destroy, incapacitate, or exploit the Nation's critical infrastructure and key resources.

Outcome

The risk to, vulnerability of, and consequence of an attack on critical infrastructure are reduced through the identification of critical infrastructure; conduct, documentation, and standardization of risk assessments; prioritization of assets; decisions regarding protective and preventative programs; and implementation of protective and preventative plans.

Relationship to National Response Plan Emergency Support Function (ESF)/Annex

This capability supports the following Emergency Support Functions (ESFs)/Annexes:

ESF #1: Transportation
ESF #2: Communications
ESF #3: Public Works and Engineering
ESF #4: Firefighting
ESF #5: Emergency Management
ESF #8: Public Health and Medical Services
ESF #10: Oil and Hazardous Materials Response
ESF #11: Agriculture and Natural Resources
ESF #12: Energy
ESF #13: Public Safety and Security
ESF #14: Long-Term Community Recovery and Mitigation
Cyber Incident Annex
Terrorism Incident Law Enforcement and Investigation Annex

Preparedness Tasks and Measures/Metrics

Activity: ***Develop and Maintain Plans, Procedures, Programs, and Systems***	
Critical Tasks	
Pro.A1a 1.1.1	Develop National Infrastructure Protection Plan (NIPP)
Pro.A1a 1.5	Establish a national CIP research and development program
Pro.A1a 1.1.2	Develop Sector-Specific Plans (SSPs)
Pro.A1a 1.1.3	Develop State and/or regional CIP Plans

Pro.A1a 1.4	Develop a national risk assessment methodology and standards for Critical Infrastructure/Key Resources (CI/KR)
Pro.A1a 1.4.1	Develop risk assessment tools
Pro.A1a 1.3.1	Establish Government Coordinating Councils (GCCs) for each sector
Pro.A1a 1.3.2	Establish Sector Coordinating Councils (SCCs) for each sector
Pro.A2a 1.1.2	Coordinate development of standard guidelines for physical security programs
Pro.A3a 1.3	Develop strategies and guidelines for cyber infrastructure protection
Pro.A2a 1.6	Develop strategies and guidelines for protection of infrastructure personnel
Pro.A1a 4.1	Define a sector-specific universe of infrastructure assets, systems, networks, and functions
Pro.A1a 3.1	Develop sector-specific security goals
Pro.A1a 1.2.1	Develop national metrics to measure progress and to assess effectiveness of the national CI/KR protection program
Pro.A1a 1.2.2	Develop sector-specific metrics to measure progress and to assess effectiveness of the sector-specific CI/KR protection programs

Preparedness Measures	**Metrics**
NIPP and SSPs are in place	Yes/No
State and/or regional CIP Plans are developed and in place	Yes/No
Appropriate risk methodology (i.e. one that takes into account the threats, consequences, and vulnerabilities) has been developed and approved by the Federal Government for CI/KR protection	Yes/No
Vulnerability assessment tool has been developed	Yes/No
GCCs have been established for each sector	Yes/No
SSPs have been reviewed by appropriate GCC	Yes/No
SCCs have been established for each sector	Yes/No
SSPs have been reviewed by appropriate SCC	Yes/No
A mechanism for coordinating CIP efforts has been established for Federal and State authorities (e.g. State, Local, and Tribal Government Coordinating Council)	Yes/No
National CIP Research and Development Plan has been established	Yes/No
CIP information-sharing mechanism has been established	Yes/No
Sector security goals have been established for each sector in partnership with security partners	Yes/No
Sector security goals support the goal of the NIPP	Yes/No
Sector security goals yield specific, measurable outcomes that allow security partners to allocate security resources and to track progress	Yes/No

Activity: *Develop and Maintain Training and Exercise Programs*	
Critical Tasks	
Pro.A1a 2.1.1	Develop and implement risk and vulnerability assessment training
Pro.A1a 2.2.1	Develop a system to "Red Team" CIP measures and technology
Pro.A2a 2.2	Develop and conduct exercise programs to test CI/KR protection plans

Preparedness Measures	Metrics
Frequency with which exercises are conducted to test the effectiveness of protective measures	Every 12 months
Vulnerability assessment training program is developed and implemented	Yes/No
Risk assessment training program is developed and implemented	Yes/No
System to "Red Team" CIP measures and technology is in place	Yes/No

Performance Tasks and Measures/Metrics

Activity: *Coordinate and Manage Critical Infrastructure Protection* **Definition: Partner/coordinate with Federal, State, local, and tribal entities, the private sector, and the international community.**	
Critical Tasks	
Pro.A1a 3.3.1	Operate public-private partnerships for Critical Infrastructure Protection (CIP) activities
Pro.A1a 3.3.2	Operate sector-specific GCCs
Pro.A1a 3.3.3	Operate sector-specific SCCs

Performance Measures	Metrics
Time in which GCC concurrence with respect to CIP is signed by all relevant parties	Within 12 months from official TCL publication
GCC concurrence includes coordination/cooperation with SCCs	Yes/No

Activity: *Identify CI/KR* **Definition: Develop an inventory of the individual assets, systems, networks, and functions that make up the Nation's CI/KR, some of which may be located outside the U.S., and collect information on them, including dependencies, interdependencies, and reliance on cyber systems.**	
Critical Tasks	
Pro.A1a 4.1.1	Develop selection criteria to identify CI/KR
Pro.A1a 4	Identify CI/KR within the Nation, region, State, or local area

Performance Measures	Metrics
Sector-specific agencies have identified assets of potential national-, regional-, or sector-level importance	Yes/No
Data have been collected on assets, systems, networks, and functions and are relevant to risk assessment efforts	Yes/No
Data have been collected on assets, systems, networks, and functions and address dependencies and interdependencies that affect functionality and performance	Yes/No
Data have been verified for accuracy	Yes/No
Frequency with which data are updated and provided to DHS	Every 12 months

Activity: *Assess Risks*

Definition: Determine which assets, systems, networks, and functions are critical by calculating risk and combining potential direct and indirect consequences of an attack (including dependencies and interdependencies associated with each identified asset), known vulnerabilities to various potential attack vectors, and general or specific threat information

Critical Tasks	
Pro.A1a 5.1	Conduct a "top-screen" consequence analysis to determine which assets, systems, networks, and functions are high consequence and therefore require risk assessment
Pro.A1a 5.3	Conduct vulnerability assessments on high-consequence assets, systems, networks, and functions
Pro.A1a 5.4	Conduct detailed threat assessments on high-consequence assets, systems, networks, and functions
Pro.A1a 5.5	Determine risk profiles of high-consequence assets, systems, networks, and functions
Pro.A1a 5.6	Conduct an interdependency analysis to determine the relationship of risks within and across sectors
Pro.A1a 5.7	Share the assessment of sector-specific infrastructure risk with interdependent entities within appropriate sectors

Performance Measures	Metrics
Procedures for analyzing threats, vulnerabilities, consequences, and risks were implemented	Yes/No
Consequence or "top-screen" analysis was performed	Yes/No
Potential threats to assets, systems, networks, and functions were identified	Yes/No
Potential threats to high-consequence assets, systems, networks, and functions were identified	Yes/No
Percent of high-consequence assets, systems, networks, and functions that have completed vulnerability assessments	100%
Percent of high-consequence assets, systems, networks, and functions that have completed a risk assessment	100%
Risk analysis results were disseminated to the proper authorities	Yes/No

Activity: *Prioritize*	
Definition: Aggregate and order assessment results to present a comprehensive picture of national CI/KR risk in order to establish protection priorities and to provide the basis for planning and the informed allocation of resources	
Critical Tasks	
Pro.A1a 6.1	Prioritize high-risk CI/KR for consideration of protective measures
Performance Measures	
CI/KR and high-consequence assets, systems, networks, and functions were normalized and prioritized for consideration of protective programs	Yes/No

Activity: *Protect*	
Definition: Select appropriate protective measures or programs and allocate resources to address targeted priorities	
Critical Tasks	
Pro.A2a 1.1.4	Develop and implement surge capacity plans to increase CIP capacity during a crisis
Pro.A2a 2.3	Implement surge capacity plans to increase CIP protection during a crisis
Pro.A2a 1.1	Develop protective programs and plans to reduce the general level of risk for the highest risk CI/KR
Pro.A2a 1.2	Develop protective programs and plans to respond to and recover from specific threat-initiated actions
Pro.A2a 5	Implement programs to defend and devalue physical CI/KR
Pro.A3a 5	Implement programs to defend and devalue critical cyber assets, systems, networks, and functions
Pro.A3a 4.1.1	Implement detection measures such as inspection surveillance, employee monitoring, and security counterintelligence
Performance Measures	**Metrics**
Percent of high-risk assets, systems, networks, and functions for which protective programs and/or mitigation strategies have been developed	100%
Percent of high-risk assets, systems, networks, and functions for which protective programs and/or mitigation strategies have been implemented	100%
Percent of high-risk assets, systems, networks, and functions that have active protective programs to measurably reduce risk	100%
Percent of high-risk assets, systems, networks, and functions for which risk has been measurably reduced	100%
Percent of high-risk assets, systems, networks, and functions for which plans for surge capacity during a crisis have been developed	100%
Percent of high-risk assets, systems, networks, and functions for which continuity of operations plans have been developed	100%

Activity: *Measure Effectiveness*	
Definition: Incorporate metrics and other evaluation procedures at the national and sector levels to measure progress and to assess effectiveness of the national CI/KR protection program	
Critical Tasks	
Pro.A1a 7.1	Collect national metrics data
Pro.A1a 7.1.1	Analyze national metrics data
Pro.A1a 7.2	Collect sector-specific metrics data
Pro.A1a 7.2.1	Analyze sector-specific metrics data

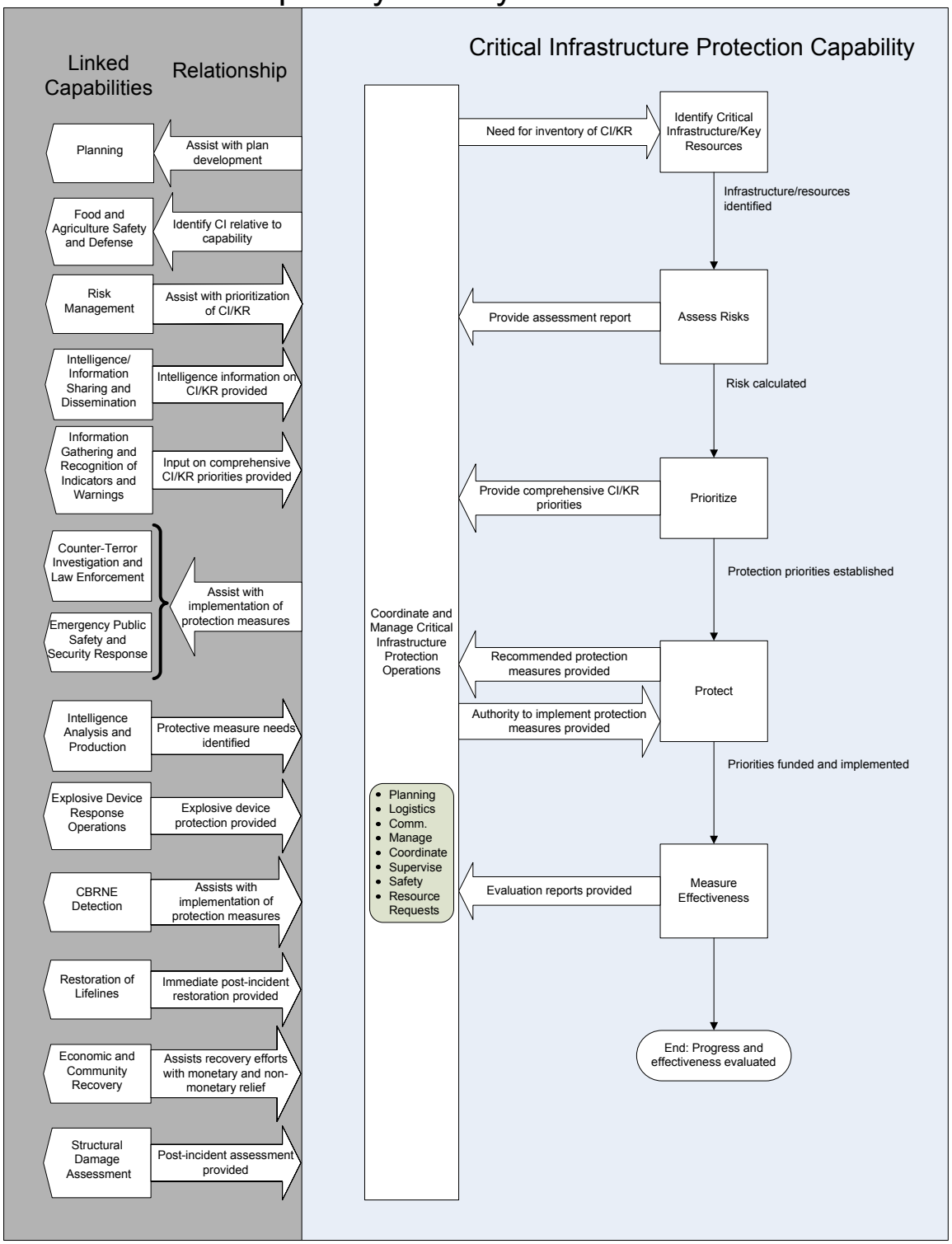
Performance Measures	**Metrics**
Frequency with which national metrics data are collected and reported	Every 12 months
Frequency with which sector-specific metrics data are collected and reported	Every 12 months

Linked Capabilities

Linked Capability	Relationship to Capability
Planning	Emergency plans developed under this capability will be coordinated with sector-specific CIP plans.
Food and Agriculture Safety and Defense	Because Food and Agriculture is one of the 17 critical infrastructure sectors, CIP provides the initial line of protection for this industry.
Risk Management	Risk Management involves the processes used to prioritize CI/KR for protection.
Intelligence and Information Sharing and Dissemination	Intelligence/information sharing mechanisms support the coordination among security partners in CIP
Information Gathering and Recognition of Indicators and Warnings	Locally generated threat and other criminal and/or terrorism-related information that results from this capability is used to establish the threat picture that forms the basis for risk in CIP
Counter-Terror Investigation and Law Enforcement	Counter-Terror Investigation and Law Enforcement are one method of deterring and thus preventing attacks on critical infrastructure.
Emergency Public Safety and Security Response	Use of law enforcement for emergency public safety and security is one form of protection for critical infrastructure assets.
Intelligence Analysis and Production	The actionable intelligence/information products produced by this capability can indicate the need for specific protective measures in CIP
Explosive Device Response Operations	Explosive Device Response Operations may involve the prevention of an explosive device at a critical asset location.
CBRNE Detection	CBRNE Detection may deter attacks on critical infrastructure or may result in the need for specific protective actions.

Linked Capability	Relationship to Capability
Restoration of Lifelines	Restoration of Lifelines addresses the immediate restoration of critical infrastructure (e.g., water, power, etc).
Economic and Community Recovery	Economic and Community Recovery includes recovery and re-building of critical infrastructure, to include greater protection.
Structural Damage Assessment	Structural Damage Assessment addresses the structural inspection of critical infrastructure to inform and prioritize mitigation resources.

Capability Activity Process Flow



Resource Element Description

Resource Elements	Components and Description
Critical Infrastructure Protection (CIP) planning personnel	
Public and private sector coordinators	
Personnel to complete vulnerability assessments	
Risk analysis personnel	
Infrastructure Security Specialists	
Infrastructure Intelligence Analysts	
National Infrastructure Protection Plan	Per Homeland Security Presidential Directive (HSPD) 7
CIP Research and Development Plan	Per HSPD 7
Sector Specific Plans	Per HSPD 7
Equipment for detection	
Equipment for protection	
Equipment for mitigation	
System to "red team" critical infrastructure protective measures and technology	

Planning Assumptions

- Critical Infrastructure Protection (CIP) may be applicable to any of the 15 National Planning Scenarios as any terrorism-related, accidental, or natural catastrophic event could disrupt or destroy CI/KR in one or more sectors. However, for purposes of determining National Targets, no scenarios were specifically considered because much of the CIP activities take place on an ongoing basis between incidents. Although protective activities are also implemented in response to particular threats or events, information regarding whether an affected asset is considered "critical" needs to be provided before any implementation can occur.
- Under the CIP process as defined in the NIPP, protection of CI/KR requires an initial determination of whether the asset/system in question and the risks being posed are "critical." Therefore, protection activities are conducted on a case-by-case basis.
- Resource needs at the State and local level may be determined through the development of a model that takes into account the presence and density of CI/KR assets in various geographic areas.
- The understanding of criticality as related to interdependent systems continues to evolve. Additional guidance will be provided as it is developed.
- State and local law enforcement is available to support CI/KR protection efforts, as required.
- Critical infrastructure information is able to be shared between Federal and State authorities and the private sector in a protected and secure way.

Target Capability Preparedness Level

Element Resource Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity Supported by Element
CIP planning personnel	Personnel	As needed	Per agency	Federal (DHS, Sector Specific Agencies)/ State	Develop and Maintain Plans, Measure Effectiveness
Public and private sector coordinators	Personnel	As needed	Per agency	Federal (DHS)	Coordinate
Public and private sector coordinators	Personnel	As needed	Per agency	Federal (Sector-Specific Agencies)/ State	Coordinate
Personnel for vulnerability assessments	Personnel	As needed	Per agency	Federal (DHS, Sector Specific Agencies)/ State	Assess Risk Prioritize
Risk analysis personnel	Personnel	As needed	Per agency	Federal (DHS, Sector Specific Agencies)/ State	Assess Risk Prioritize
Infrastructure Security Specialists	Personnel	As needed	Per agency	Federal (DHS, Sector Specific Agencies)/ State	Protect
Infrastructure Intelligence Analysts	Personnel	As needed	Per agency	Federal (DHS, Sector Specific Agencies)/ State	Assess Risk
National Infrastructure Protection Plan	Planning	1	Nationally	Federal (DHS)	All activities
CIP Research and Development Plan	Planning	1	Nationally	Federal (DHS)	All activities
Sector-Specific Plans	Planning	1	Per Sector-Specific Agency	Federal (Sector Specific Agencies)	All activities
Equipment for detection	Equipment	As needed	Per asset	Federal/State/ Local	Protect
Equipment for protection	Equipment	As needed	Per asset	Federal/State/ Local	Protect
Equipment for mitigation	Equipment	As needed	Per asset	Federal/State/ Local	Protect
System to Red Team critical infrastructure protective measures and	Exercises			Federal	All Activities

Element Resource Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity Supported by Element
technology					

References

1. National Infrastructure Protection Plan. Department of Homeland Security. June 2006.
2. Homeland Security Presidential Directive/HSPD–8: National Preparedness. The White House, Office of the Press Secretary. December 2003. http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html.
3. Homeland Security Presidential Directive /HSPD–7: Critical Infrastructure Identification, Prioritization, and Protection. The White House, Office of the Press Secretary. December 2003. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
4. National Response Plan. U.S. Department of Homeland Security. December 2004.
5. National Incident Management System. U.S. Department of Homeland Security. March 2004. http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf.
6. Department of Homeland Security Sector-Specific Intelligence Sharing Analysis Center (ISAC) Information. Executive Order 13356, State and Local Tiger Team. U.S. Department of Homeland Security. 2004. http://a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/pdf/04-20052.pdf.
7. The Office for Domestic Preparedness Guidelines for Homeland Security: Prevention and Deterrence. U.S. Department of Homeland Security, Office for Domestic Preparedness. June 2003. http://www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf.
8. Applying Security Practices to Justice Information Sharing. U.S. Department of Justice, Global Justice Information Sharing Initiative, Security Working Group. March 2004. http://it.ojp.gov/documents/200404_ApplyingSecurityPractices_v_2.0.pdf.
9. The National Criminal Intelligence Sharing Plan. U.S. Department of Justice, Global Justice Information Sharing Initiative. Revised June 2005. http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf.
10. Homeland Security Information Network. U.S. Department of Homeland Security. http://www.dhs.gov/dhspublic/display?theme=43&content=3747&print=true.
11. Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO–03–1165T. U.S. General Accounting Office. September 2003. http://www.gao.gov/new.items/d031165t.pdf.
12. Information/Intelligence Sharing System Survey. U.S. Department of Justice, Global Justice Information Sharing Initiative, Global Intelligence Working Group. 2003. http://it.ojp.gov/documents/intell_sharing_system_survey.pdf.
13. National Strategy for Homeland Security. Office of Homeland Security, The White House. July 2002. http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf.
14. Risk Management: An Essential Guide to Protecting Critical Assets. National Infrastructure Protection Center. November 2002.
15. The 9/11 Commission Report. National Commission on Terrorist Attacks upon the United States. July 2004. http://www.9-11commission.gov/report/911Report.pdf.
16. National Strategy for Transportation Security. U.S. Department of Homeland Security.
17. National Fire Protection Association Codes and Standards. http://www.nfpa.org/aboutthecodes/list_of_codes_and_standards.asp